

Datenschutzerklärung / Privacy Policy

NOTE: English translation is available for informational purposes only and is written after the legally binding German version. (see §15)

Diese Erklärung ergänzt das Impressum (aufrufbar unter <https://neoprotect.net/imprint>) und die AGB (aufrufbar unter <https://neoprotect.net/terms>).

Mit der folgenden Datenschutzerklärung möchten wir Sie darüber aufklären, welche Arten Ihrer personenbezogenen Daten wir zu welchen Zwecken und in welchem Umfang verarbeiten.

Die Datenschutzerklärung gilt für alle von uns durchgeführten Verarbeitungen personenbezogener Daten, sowohl im Rahmen der Erbringung unserer Leistungen als auch insbesondere auf unseren Webseiten, in mobilen Applikationen sowie innerhalb externer Onlinepräsenzen, wie z. B. unserer Social-Media-Profile (nachfolgend zusammenfassend bezeichnet als „Onlineangebot“). Zum Onlineangebot zählt ebenfalls unser passwortgeschützter Mitgliederbereich (nachfolgend „Panel“).

Die verwendeten Begriffe sind nicht geschlechtsspezifisch.

§1 Verantwortlicher

Verantwortlicher im Sinne der DSGVO und des BDSG ist:

NeoProtect GmbH
Ulrichsberger Straße 17
94469, Deggendorf
Deutschland

Amtsgericht: Deggendorf HRB 6544
Sitz: Deggendorf
Geschäftsführer: Kilian Pronold, Noah Kolossa
E-Mail: dataprotection@neoprotect.net
Telefon: +49 991 99993744
Website: <https://neoprotect.net>

§2 Datenschutzbeauftragter

Nach aktuellem Stand ist kein Datenschutzbeauftragter (DSB) bestellt.
Datenschutzrechtliche Anfragen richten Sie bitte direkt an die unter Ziffer 1 genannte Kontaktadresse. Wir überprüfen fortlaufend, ob die gesetzliche Bestellpflicht gemäß Art. 37 DSGVO i. V. m. § 38 BDSG für unser Unternehmen eintritt.

§3 Registrierung und Nutzerkonto

3.1 Erhobene Daten

Bei der Registrierung für unser Onlineangebot verarbeiten wir folgende personenbezogene Daten:

- Vor- und Nachname
- E-Mail-Adresse
- Passwort (ausschließlich in verschlüsselter Form (Hash) gespeichert)
- Unternehmensname und -adresse (sofern angegeben)
- IP-Adresse und Zeitstempel der Registrierung

3.2 Zweck und Rechtsgrundlage

Die Verarbeitung dient der Begründung und Durchführung des Nutzungsvertrages (Art. 6 Abs. 1 lit. b DSGVO) sowie der Erfüllung rechtlicher Verpflichtungen (Art. 6 Abs. 1 lit. c DSGVO).

3.3 Einwilligungsprotokoll bei der Registrierung

Im Zuge der Registrierung stimmen Sie ausdrücklich unseren Allgemeinen Geschäftsbedingungen (AGB) sowie dieser Datenschutzerklärung zu. Diese Einwilligung wird mit Zeitstempel und IP-Adresse protokolliert. Sie kann jederzeit mit Wirkung für die Zukunft widerrufen werden; die Rechtmäßigkeit der bis zum Widerruf erfolgten Verarbeitung bleibt hiervon unberührt.

3.4 Speicherdauer

Kontodaten werden für die Dauer des Nutzungsverhältnisses gespeichert. Eine Löschung des Benutzerkontos und der damit verbundenen personenbezogenen Daten erfolgt ausschließlich auf ausdrücklichen Antrag des Nutzers, welcher entweder über die Kontoeinstellungen oder durch schriftliche Anfrage an dataprotection@neoprotect.net gestellt werden kann. Nach Eingang eines Löschantrags wird das Konto innerhalb der gesetzlichen Frist vollständig gelöscht, sofern keine gesetzlichen Aufbewahrungsfristen entgegenstehen. Daten, die gesetzlichen Aufbewahrungspflichten unterliegen (z. B. Rechnungsdaten gemäß § 147 AO), werden bis zum Ablauf der jeweiligen Frist gespeichert und anschließend gelöscht.

§4 Nutzung des Onlineangebots und des Panels

Bei der Nutzung unseres Onlineangebots werden technische Zugriffsdaten automatisch erfasst. Diese umfassen IP-Adresse, Browsertyp und -version, Betriebssystem, aufgerufene Seiten und Funktionen, Datum und Uhrzeit des Zugriffs sowie Session-IDs. Die Verarbeitung erfolgt zur Sicherstellung des technischen Betriebs, zur Fehlerbehebung und zum Schutz vor missbräuchlicher Nutzung (Art. 6 Abs. 1 lit. f DSGVO). Eine Zusammenführung mit anderen personenbezogenen Daten findet nur statt, soweit dies für Sicherheit oder Vertragsdurchführung erforderlich ist.

§5 KI-gestützter Chatbot (Amazon Bedrock / Claude)

5.1 Allgemeines und Transparenz

Der KI-gestützte Assistent ist ein zentraler Kommunikationskanal unseres Kundensupports und auf unserem Onlineangebot sowohl auf öffentlich zugänglichen Seiten als auch innerhalb des Panels verfügbar. Bei Beginn einer Supportanfrage wird der Support regelmäßig zunächst über den KI-gestützten Assistenten bereitgestellt. Nicht registrierte Nutzer sowie registrierte Nutzer, die dem KI-Einsatz nicht zugestimmt haben, können den Support alternativ ohne Nutzung des KI-Assistenten per E-Mail über die auf unserer Website angegebenen Adressen in Anspruch nehmen. Einzelheiten zur Rechtsgrundlage und zu den Alternativen ergeben sich aus Abschnitt 5.4.

Der Chatbot wird bei jeder Interaktion unmissverständlich als KI-System gekennzeichnet – es handelt sich zu keiner Zeit um eine Konversation mit einem menschlichen Mitarbeiter. Diese Kennzeichnungspflicht ergibt sich aus Art. 50 Abs. 1 der KI-Verordnung (Verordnung (EU) 2024/1689, „EU AI Act“) sowie dem Transparenzgrundsatz nach Art. 5 Abs. 1 lit. a i. V. m. Art. 13 DSGVO / GDPR.

Vor der ersten Nutzung wird ein Hinweis eingeblendet, der über den KI-Einsatz sowie die damit verbundene Datenverarbeitung informiert und auf diese Datenschutzerklärung verweist. Die Inanspruchnahme des Supports setzt die Kenntnisnahme dieses Hinweises voraus.

Empfehlung: Bitte geben Sie im Chatbot keine besonders sensiblen personenbezogenen Daten ein – insbesondere keine Gesundheitsdaten, Bankverbindungen, Ausweisdaten oder Passwörter.

5.2 Technologieanbieter

Wir nutzen für den Betrieb des Chatbots den Dienst **Amazon Bedrock** der Amazon Web Services EMEA SARL (siehe Abschnitt 8.5 und 10). Über Amazon Bedrock werden Sprachmodelle von Anthropic (Claude) ausgeführt. Die Verarbeitung erfolgt ausschließlich auf AWS-Infrastruktur; Anthropic hat keinen direkten Zugriff auf die im Rahmen der Chatbot-Nutzung übermittelten Daten. Der mit AWS abgeschlossene AVV gemäß Art. 28 DSGVO / GDPR umfasst auch die Nutzung von Amazon Bedrock.

5.3 Verarbeitende Daten

Im Rahmen der Chatbot-Nutzung werden folgende Daten an den Dienst übermittelt:

- Ihre Eingaben (Nachrichten und Anfragen) im Chat
- Sitzungsbezogene Kontextinformationen, soweit für die Antwortgenerierung erforderlich
- Metadaten (Zeitstempel, Session-ID)
- Technische Service-Konfigurationsdaten zur Fehlererkennung des Dienstes (keine personenbezogenen Daten)

Bei nicht eingeloggten Nutzern werden keine darüber hinausgehenden personenbezogenen Daten verarbeitet oder mit einem Nutzerkonto verknüpft.

5.4 Rechtsgrundlage

Für **eingeloggte Nutzer** erfolgt die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO. Unser berechtigtes Interesse liegt in der effizienten, skalierbaren und qualitativ

einheitlichen Erbringung des Kundensupports durch den Einsatz eines KI-gestützten Assistenzsystems. Der Chatbot ist dabei kein zwingender Vertragsbestandteil, sondern ein empfohlener Kommunikationskanal; alternative Kontaktmöglichkeiten stehen über die auf unserer Website angegebenen E-Mail-Adressen zur Verfügung.

Wir haben im Rahmen einer dokumentierten Interessenabwägung berücksichtigt, dass (i) die Verarbeitung auf das für die Supporterbringung Erforderliche beschränkt ist, (ii) keine automatisierten Entscheidungen im Sinne von Art. 22 DSGVO getroffen werden, (iii) der Nutzer über den KI-Einsatz vorab transparent informiert wird und (iv) Chat-Verläufe auf Antrag jederzeit gelöscht werden können. Ihr Recht auf Widerspruch gemäß Art. 21 DSGVO bleibt hiervon unberührt.

Für **nicht eingeloggte Nutzer** erfolgt die Verarbeitung auf Grundlage der ausdrücklich erteilten Einwilligung gemäß Art. 6 Abs. 1 lit. a DSGVO.

Vor der ersten Nutzung des Chatbots wird nicht eingeloggten Nutzern ein Hinweis eingeblendet, der über den KI-Einsatz, die verarbeiteten Daten sowie die Sitzungsbeschränkung der Speicherung informiert und auf diese Datenschutzerklärung verweist. Die Nutzung des Chatbots kann erst nach aktiver Bestätigung dieses Hinweises erfolgen. Die Einwilligung wird sitzungsbezogen protokolliert. Sie kann jederzeit durch Beenden der Sitzung oder durch Nichtnutzung des Chatbots verweigert bzw. widerrufen werden; eine dauerhafte Zuordnung zu einer Person findet ohne Registrierung nicht statt.

Für eingeloggte Nutzer wird vor der ersten Nutzung ebenfalls ein Hinweis eingeblendet, der über den KI-Einsatz informiert und auf diese Datenschutzerklärung verweist.

5.5 Drittlandübermittlung

Wir nutzen Amazon Bedrock mit einem regionsgebundenen Endpunkt in der AWS-Region eu-central-1 (Frankfurt, Deutschland); ein regionsübergreifendes oder globales Routing der Inferenz ist für diesen Dienst deaktiviert. Die Verarbeitung der Chatbot-Inhalte (Prompts und Antworten) findet dadurch innerhalb des Europäischen Wirtschaftsraums statt. Die über Amazon Bedrock bereitgestellten Modelle von Anthropic laufen auf AWS-verwalteter Infrastruktur; Anthropic hat keinen Zugriff auf die im Rahmen der Chatbot-Nutzung übermittelten Inhalte (siehe Abschnitt 5.2). Ein Restrisiko eines behördlichen Zugriffs auf Grundlage US-amerikanischer Gesetze (insbesondere des CLOUD Act) lässt sich bei einem US-Konzern als Betreiber der Infrastruktur nicht vollständig ausschließen; wir begegnen diesem Risiko durch die mit AWS vereinbarten Garantien und technische Schutzmaßnahmen (siehe Abschnitt 10). Soweit für ergänzende technische Verarbeitungen (z. B. Betrieb, Fehlerbehebung oder Support) im Einzelfall eine Übermittlung in ein Drittland erforderlich ist, erfolgt diese nur auf Grundlage der in Abschnitt 10 genannten Garantien.

5.6 Automatisierte Entscheidungsfindung

Der Chatbot trifft keine rechtlich bindenden oder Sie in vergleichbarer Weise erheblich beeinträchtigenden automatisierten Entscheidungen im Sinne von Art. 22 DSGVO / GDPR. Alle generierten Antworten sind als Informationsangebote zu verstehen und ersetzen keine rechtliche, medizinische oder fachliche Beratung.

5.7 Speicherdauer

Chat-Verläufe eingeloggter Nutzer werden für die Dauer des Nutzungsverhältnisses gespeichert, maximal jedoch 3 Jahre. Eine Löschung erfolgt auf ausdrücklichen Antrag über die Kontoeinstellungen oder per E-Mail an support@neoprotect.net mit dem Betreff „GDPR Data removal“; nach Eingang des Antrags erfolgt die Löschung innerhalb der gesetzlichen Frist.

Chat-Verläufe nicht eingeloggter Nutzer werden ausschließlich für die Dauer der Sitzung verarbeitet und nicht dauerhaft gespeichert. Nach Beendigung der Sitzung werden die Gesprächsdaten gelöscht.

§6 Zahlungsabwicklung

6.1 Stripe

Für die Zahlungsabwicklung nutzen wir:

Stripe Payments Europe, Ltd. 1 Grand Canal Street Lower, Grand Canal Dock, Dublin D02 H210, Irland Datenschutzinformationen: <https://stripe.com/de/privacy>

Ihre Zahlungsdaten (z. B. Kreditkartennummer, IBAN) werden direkt an Stripe übermittelt; wir selbst speichern keine vollständigen Zahlungsdaten. Stripe handelt für Teile der Verarbeitung als eigenverantwortliche Stelle. Für Drittlandübermittlungen in die USA stützt sich Stripe auf das EU-U.S. Data Privacy Framework (DPF) sowie SCCs. Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO.

6.2 PayPal

Alternativ bieten wir die Zahlung über PayPal an:

PayPal (Europe) S.à r.l. et Cie, S.C.A. 22-24 Boulevard Royal, L-2449 Luxemburg
Datenschutzinformationen: <https://www.paypal.com/de/webapps/mpp/ua/privacy-full>

Bei Auswahl von PayPal werden Sie auf deren Plattform weitergeleitet. PayPal verarbeitet Ihre personenbezogenen Daten als eigenverantwortliche Stelle. Konzerninterner Transfer in die USA erfolgt auf Basis von DPF und SCCs. Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO.

§7 Interne Tools und Auftragsvertreter

Wir setzen die nachfolgenden Softwaretools ein, auf die ausschließlich Mitarbeiter der NeoProtect GmbH Zugriff haben. Sämtliche Mitarbeiter sind durch Vertraulichkeitsvereinbarungen (NDAs) zur Verschwiegenheit verpflichtet. Diese Maßnahme ist Bestandteil unserer technisch-organisatorischen Schutzmaßnahmen gemäß Art. 32 DSGVO.

Neben festangestellten Mitarbeitern setzen wir in begrenztem Umfang externe Auftragnehmer (Freelancer) ein, die im Rahmen ihrer Tätigkeit ähnliche Zugriffe auf interne Systeme und – soweit für ihre Aufgaben erforderlich – auf personenbezogene Daten haben können wie Mitarbeiter. Mit diesen Personen werden Auftragsverarbeitungsverträge gemäß Art. 28 DSGVO sowie Vertraulichkeitsvereinbarungen (NDAs) abgeschlossen. Der Zugriff erfolgt ausschließlich nach dem Need-to-know-Prinzip. Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO.

7.1 Slack (interne Kommunikation)

Slack (Betreiber: Salesforce, Inc., 415 Mission Street, San Francisco, CA 94105, USA) wird ausschließlich zur internen Kommunikation genutzt. Im Rahmen von Support-Prozessen können dabei mittelbar personenbezogene Daten zu Nutzeranfragen besprochen werden. Mit Salesforce/Slack besteht ein AVV nach Art. 28 DSGVO; Drittlandübermittlungen in die USA erfolgen auf Basis von DPF und SCCs. Datenschutzinformationen: <https://slack.com/trust/privacy>. Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an effizienter interner Kommunikation).

7.2 Google Workspace (E-Mail, Dokumente, Kalender, Telefonie) und Google Places API (Adressen Validierung)

Google Workspace (Betreiber: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland; Tochtergesellschaft der Google LLC, USA) nutzen wir für E-Mail, Dokumentenbearbeitung, Kalender sowie Telefonie und Sprachkommunikation. Dabei können personenbezogene Daten in geschäftlicher Kommunikation enthalten sein. Darüber hinaus nutzen wir die Google Places API (Google Maps Plattform) zur serverseitigen Validierung von Adresseingaben. Dabei werden eingegebene Adressdaten ausschließlich von unserem Server an die Google-API übermittelt; eine direkte Verbindung zwischen Ihrem Browser und Google-Servern findet im Rahmen dieser Funktion nicht statt. Es werden nur die zur Adressvalidierung notwendigen Daten (eingegebene Adressbestandteile) übermittelt – keine darüber hinausgehenden personenbezogenen Daten.

Mit Google besteht ein AVV nach Art. 28 DSGVO; Drittlandübermittlungen in die USA erfolgen auf Basis von DPF und SCCs. Datenschutzinformationen: <https://policies.google.com/privacy>. Rechtsgrundlage: Art. 6 Abs. 1 lit. b und lit. f DSGVO.

7.3 Linear (Projektmanagement)

Linear (Betreiber: Linear Orbit Inc., USA) nutzen wir zur internen Aufgaben- und Projektverwaltung. Tickets können mittelbar personenbezogene Daten zu Nutzeranfragen enthalten. Mit Linear besteht ein AVV nach Art. 28 DSGVO; Drittlandübermittlungen in die USA erfolgen auf Basis von SCCs. Datenschutzinformationen: <https://linear.app/privacy>. Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an effizientem Projektmanagement).

7.4 Lexoffice / Lexware (Buchhaltung und Rechnungsstellung)

Lexoffice (Betreiber: Lexware GmbH & Co. KG bzw. Haufe-Lexware GmbH & Co. KG, Munzinger Straße 9, 79111 Freiburg im Breisgau, Deutschland) nutzen wir zur Buchhaltung sowie zur Erfüllung steuer- und handelsrechtlicher Aufzeichnungspflichten. Dabei verarbeiten wir Stammdaten unserer Kunden (Name, Anschrift, ggf. USt-IdNr.) sowie Rechnungs- und Zahlungsdaten.

Die Datenverarbeitung erfolgt auf Servern in Deutschland; eine Drittlandübermittlung findet nicht statt. Mit Lexware besteht ein Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO.

Datenschutzinformationen: <https://www.lexware.de/datenschutz/>.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragsdurchführung) sowie Art. 6 Abs. 1 lit. c DSGVO i. V. m. § 147 AO, § 257 HGB (Erfüllung gesetzlicher Aufbewahrungs- und Aufzeichnungspflichten).

7.5 DocuSeal (elektronische Signatur und Dokumentenverwaltung)

DocuSeal (Betreiber: DocuSeal LLC, 332 S Michigan Ave, Suite 121 #5896, Chicago IL 60604) nutzen wir zur Erstellung, Versendung und rechtssicheren elektronischen Signatur von Dokumenten (z. B. Verträge, Auftragsbestätigungen, NDAs). Dabei verarbeiten wir Stammdaten der unterzeichnenden Personen (insbesondere Name, E-Mail-Adresse, ggf. Unternehmensbezug) sowie die Dokumenteninhalte und Signaturmetadaten (z. B. Zeitstempel, IP-Adresse zum Zeitpunkt der Signatur).

Wir setzen die europäische Variante (docuseal.eu) ein; die Datenverarbeitung erfolgt auf Servern innerhalb der EU/des EWR, eine Drittlandübermittlung findet nicht statt. Mit DocuSeal besteht ein Auftragsverarbeitungsvertrag (AVV) gemäß Art. 28 DSGVO.

Datenschutzinformationen: <https://www.docuseal.com/privacy>.

Rechtsgrundlage: Art. 6 Abs. 1 lit. b DSGVO (Vertragsdurchführung) sowie Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an einer effizienten und rechtssicheren elektronischen Dokumentenabwicklung).

§8 Hosting und technische Infrastruktur

Zum Betrieb unseres Onlineangebots setzen wir externe Hosting- und Infrastrukturanbieter ein, auf deren Servern bzw. Netzwerken personenbezogene Daten (z. B. Server-Logs, hochgeladene Dateien, Datenbankinhalte) gespeichert oder durchgeleitet werden. Mit allen nachfolgend genannten Anbietern haben wir Auftragsverarbeitungsverträge (AVV) gemäß Art. 28 DSGVO abgeschlossen.

8.1 Hetzner (primäre Serverinfrastruktur)

Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Deutschland

Datenschutzinformationen: <https://www.hetzner.com/de/legal/privacy-policy>

Hetzner ist ein deutsches Unternehmen mit Rechenzentren ausschließlich in Deutschland und Finnland (EU/EWR). Es findet keine Drittlandübermittlung personenbezogener Daten statt. Auf den Hetzner-Servern können Datenbankinhalte, Anwendungsdaten und Server-Logs gespeichert sein. Rechtsgrundlage: Art. 6 Abs. 1 lit. b und lit. f DSGVO.

8.2 OVHcloud (Serverinfrastruktur)

OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken, Deutschland (Tochtergesellschaft der OVH SAS, 2 rue Kellermann, 59100 Roubaix, Frankreich) Datenschutzinformationen:

<https://www.ovhcloud.com/de/personal-data-protection/>

OVHcloud betreibt Rechenzentren in Deutschland, Frankreich und weiteren EU/EWR-Standorten. Eine Drittlandübermittlung außerhalb des EWR findet standardmäßig nicht statt. Auf OVH-Infrastruktur können Anwendungsdaten und Backups gespeichert sein. Rechtsgrundlage: Art. 6 Abs. 1 lit. b und lit. f DSGVO.

8.3 Cloudflare (CDN und Netzwerksicherheit)

Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA

Datenschutzinformationen: <https://www.cloudflare.com/de-de/privacypolicy/>

Wir nutzen Cloudflare als Content Delivery Network (CDN) zur schnelleren Auslieferung unserer Webinhalte sowie zum Schutz vor DDoS-Angriffen und sonstigen Bedrohungen. Der Traffic zwischen Ihrem Browser und unserem Onlineangebot wird dabei über das globale Netzwerk von Cloudflare geleitet; Cloudflare kann dabei technische Zugriffsdaten (insbesondere IP-Adressen) verarbeiten. Die Drittlandübermittlung in die USA erfolgt auf Basis des DPF sowie der SCCs gemäß Art. 46 Abs. 2 lit. c DSGVO. Für Nutzer im EWR werden personenbezogene Daten bevorzugt in europäischen Rechenzentren verarbeitet. Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an sicherer und performanter Bereitstellung des Onlineangebots).

8.4 hCaptcha (Bot- und Missbrauchserkennung)

Intuition Machines, Inc., 350 Alabama St, San Francisco, CA 94110, USA

Datenschutzinformationen: <https://www.hcaptcha.com/privacy>

Zum Schutz unserer Formulare (insbesondere Registrierung und Login) vor automatisierten Zugriffen, Bots und Missbrauch setzen wir den Dienst hCaptcha der Intuition Machines, Inc. ein. Bei der Nutzung von hCaptcha analysiert der Dienst automatisiert das Verhalten des Besuchers anhand verschiedener Merkmale (insbesondere IP-Adresse, Browser- und Geräteinformationen sowie Interaktionsdaten wie Mausbewegungen), um zwischen menschlichen Nutzern und automatisierten Anfragen zu unterscheiden. Die Analyse erfolgt im Hintergrund; hierzu wird ein Skript von den Servern von hCaptcha geladen, wodurch technische Zugriffsdaten (insbesondere Ihre IP-Adresse) an Intuition Machines übermittelt werden. Die Drittlandübermittlung in die USA erfolgt auf Basis des EU-U.S. Data Privacy Frameworks (DPF) sowie ergänzend der Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO. Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse am Schutz unseres Onlineangebots vor Bots, Spam und missbräuchlicher automatisierter Nutzung).

8.5 Amazon Web Services - AWS (CDN und Objektspeicher)

Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, L-1855 Luxemburg (Tochtergesellschaft der Amazon.com, Inc., 410 Terry Ave. North, Seattle, WA 98109, USA)

Datenschutzinformationen: <https://aws.amazon.com/de/privacy/>

Wir nutzen AWS als Content Delivery Network (Amazon CloudFront) für die performante Auslieferung statischer Inhalte, als Objektspeicher (Amazon S3) für die sichere Ablage von Dateien und Medien sowie als KI-Inferenz-Infrastruktur (Amazon Bedrock) für den Betrieb des Chatbots (siehe Abschnitt 5). Auch nutzen wir AWS für die Speicherung etwaiger Software-Versionen unserer Produkte (Amazon ECR) um autonome Versionsverwaltung zu realisieren als auch für interne Proxy-Tätigkeiten für u.a. interne SSH- und VPN-Dienste (Amazon EC2) um selbst gesetzte Sicherheitsstandards einzuhalten. Wir setzen AWS-Dienste primär in der Region eu-central-1 (Frankfurt, Deutschland) ein. Drittlandübermittlungen in die USA können im Rahmen der konzerninternen Infrastruktur nicht vollständig ausgeschlossen werden; sie erfolgen auf Basis des DPF sowie der SCCs gemäß Art. 46 Abs. 2 lit. c DSGVO / GDPR. Rechtsgrundlage: Art. 6 Abs. 1 lit. b und lit. f DSGVO / GDPR.

8.6 Atlassian Statuspage (Statusseite, Systemstatusanzeige)

Atlassian Network Services, Inc., 350 Bush Street, Floor 13, San Francisco, CA 94104, USA

Datenschutzinformationen: <https://www.atlassian.com/legal/privacy-policy>

Beim Laden unseres Panels werden Statusinformationen von den Servern von Atlassian abgerufen und auf unserer Seite dargestellt. Dabei kann Ihr Browser eine direkte Verbindung zu Atlassians Infrastruktur aufbauen, wodurch Atlassian technische Zugriffsdaten – insbesondere Ihre IP-Adresse – verarbeiten kann.

Wir übermitteln selbst keine personenbezogenen Daten an Atlassian. Sofern Sie sich für E-Mail-Benachrichtigungen zu Statusänderungen anmelden möchten, erfolgt dies ausschließlich durch Ihre freiwillige Eingabe auf der Atlassian-Statuspage; die Verarbeitung dieser Daten liegt im alleinigen Verantwortungsbereich von Atlassian.

Da Atlassian seinen Sitz in den USA hat, kann es bei der Datenverarbeitung zu einer Drittlandübermittlung kommen. Diese erfolgt auf Basis der Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO sowie des EU-U.S. Data Privacy Frameworks (DPF).

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an der transparenten Kommunikation des Systemstatus gegenüber unseren Nutzern).

§9 Präsenzen in Sozialen Netzwerken

Wir unterhalten öffentliche Profile auf den nachfolgend genannten sozialen Netzwerken und veröffentlichen dort organische Inhalte sowie bezahlte Werbeanzeigen. Eine technische Einbindung dieser Plattformen in unser Onlineangebot (z. B. durch Plugins, Tracking-Pixel oder Social-Buttons) findet nicht statt.

Sobald Sie die jeweiligen Plattformen besuchen oder mit unseren Profilen interagieren, verarbeiten die Plattformbetreiber Ihre personenbezogenen Daten eigenverantwortlich nach ihren eigenen Datenschutzrichtlinien. Auf diese Verarbeitung haben wir keinen Einfluss. Wir empfehlen, die Datenschutzhinweise der jeweiligen Plattformen zu lesen.

9.1 Instagram und Facebook (Meta Platforms)

Meta Platforms Ireland Limited 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland
Datenschutzinformationen: <https://www.facebook.com/privacy/policy>

Wir veröffentlichen auf unseren Meta-Seiten (Instagram und Facebook) organische Beiträge sowie bezahlte Werbeanzeigen. Im Rahmen der Werbeschaltung nutzt Meta eigene Targeting-Mechanismen auf Basis der bei Meta gespeicherten Nutzerdaten; wir übermitteln dabei keine personenbezogenen Daten unserer eigenen Nutzer an Meta. Für die Verarbeitung von Seitenstatistiken (Page Insights) besteht eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO zwischen uns und Meta. Die wesentlichen Inhalte der Vereinbarung sind unter https://www.facebook.com/legal/terms/page_controller_addendum einsehbar. Meta nimmt dabei die primäre Verantwortung für die Erfüllung von Betroffenenrechten in Bezug auf Page-Insights-Daten wahr. Ungeachtet dessen können Sie Ihre Rechte auch uns gegenüber geltend machen; wir leiten Ihr Anliegen ggf. an Meta weiter. Drittlandübermittlungen in die USA erfolgen über das EU-U.S. Data Privacy Framework (Angemessenheitsbeschluss, Art.

45 DSGVO) und, soweit einschlägig, ergänzend über Standardvertragsklauseln (Art. 46 DSGVO). Rechtsgrundlage für die Verarbeitung ist Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse liegt in der Außendarstellung und Kommunikation unseres Unternehmens.

9.2 LinkedIn

LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Irland

Datenschutzinformationen: <https://www.linkedin.com/legal/privacy-policy>

Wir veröffentlichen auf unserer LinkedIn-Unternehmensseite organische Inhalte sowie bezahlte Anzeigen (LinkedIn Ads). Für Seitenstatistiken (Page Analytics) besteht eine gemeinsame Verantwortlichkeit gemäß Art. 26 DSGVO mit LinkedIn Ireland.

Drittlandübermittlungen in die USA erfolgen über DPF und SCCs. Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO.

Die wesentlichen Inhalte der Vereinbarung über die gemeinsame Verantwortlichkeit sind unter <https://www.linkedin.com/legal/page-joint-controller-addendum> einsehbar.

9.3 X (vormals Twitter)

Wir unterhalten ein öffentliches Profil auf der Plattform X. Betreiber für Nutzer im EWR ist die Twitter International Unlimited Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Irland (Muttergesellschaft: X Corp., USA). Datenschutzinformationen:

<https://x.com/de/privacy>. Sobald Sie unser Profil besuchen oder mit unseren Beiträgen interagieren, verarbeitet der Plattformbetreiber Ihre personenbezogenen Daten eigenverantwortlich nach seinen eigenen Datenschutzrichtlinien; auf diese Verarbeitung haben wir keinen Einfluss. Eine technische Einbindung in unser Onlineangebot (Plugins, Tracking-Pixel, Social-Buttons) findet nicht statt. Drittübermittlungen in die USA erfolgen auf Basis der Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO.

Rechtsgrundlage: Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an öffentlicher Außendarstellung und Kommunikation).

9.4 Discord

Wir betreiben einen öffentlichen Discord-Server, der unseren Nutzern als Community- und Support-Kanal dient. Betreiber ist die Discord Netherlands BV (europäische Niederlassung; Muttergesellschaft: Discord Inc., 444 De Haro Street, San Francisco, CA 94107, USA).

Datenschutzinformationen: <https://discord.com/privacy>. Wenn Sie unserem Server beitreten oder dort kommunizieren, verarbeitet Discord die dabei anfallenden Daten (insbesondere Nutzernamen, Nutzer-ID, Nachrichteninhalte, Verbindungsdaten) als eigenverantwortliche Stelle nach seinen eigenen Datenschutzrichtlinien. Soweit wir den Server administrieren und in diesem Rahmen personenbezogene Daten verarbeiten (z. B. zur Beantwortung von Anfragen oder zur Moderation), erfolgt dies auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO (berechtigtes Interesse an Community-Betreuung und Support); die Teilnahme ist freiwillig. Bitte geben Sie im Chat keine besonders sensiblen Daten ein. Drittübermittlungen in die USA erfolgen auf Basis der Standardvertragsklauseln (SCCs) gemäß Art. 46 Abs. 2 lit. c DSGVO.

9.5 Hinweise zur Werbeschaltung

Bei der Schaltung von Werbeanzeigen übermitteln wir den Plattformen ausschließlich aggregierte Zielgruppendefinitionen (z. B. Branche, Interessen, geografische Region) –

keine personenbezogenen Einzeldaten unserer Nutzer oder Kunden. Die Plattformen spielen unsere Anzeigen anhand dieser Vorgaben ihrer eigenen Nutzerbasis aus. Für Fragen zur plattformseitigen Datenverarbeitung verweisen wir auf die jeweiligen Datenschutzhinweise.

§10 Drittlandübermittlungen

Mehrere der von uns eingesetzten Anbieter haben ihren Sitz in den USA. Übermittlungen in die USA stützen wir – je nach Anbieter – auf eine der beiden folgenden Grundlagen: (i) das EU-U.S. Data Privacy Framework, für das die EU-Kommission am 10. Juli 2023 einen Angemessenheitsbeschluss nach Art. 45 DSGVO gefasst hat, sofern der jeweilige Empfänger aktiv unter dem DPF zertifiziert ist; oder (ii) die Standardvertragsklauseln der EU-Kommission als geeignete Garantien nach Art. 46 DSGVO, ergänzt durch technische und organisatorische Schutzmaßnahmen. Die jeweils einschlägige Transfer-Rechtsgrundlage je Anbieter ergibt sich aus der nachstehenden Tabelle.

Anbieter	Sitz	Transfer-Rechtsgrundlage
Hetzner Online GmbH	Deutschland (EU)	Kein Drittlandtransfer
OVH GmbH / OVH SAS	Deutschland / Frankreich (EU)	Kein Drittlandtransfer
Cloudflare, Inc.	USA	DPF + SCCs
Intuition Machines, Inc. (hCaptcha)	USA	DPF + SCCs
Amazon Web Services EMEA	Luxemburg / USA	DPF + SCCs
Anthropic, PBC	USA	SCCs (Art. 46 Abs. 2 lit. c DSGVO)
Meta Platforms Ireland	Irland / USA	DPF + SCCs
LinkedIn Ireland	Irland / USA	DPF + SCCs
Stripe Payments Europe	Irland / USA	DPF + SCCs
PayPal (Europe)	Luxemburg / USA	DPF + SCCs
Salesforce / Slack	USA	DPF + SCCs
Google LLC / Google Ireland	USA / Irland	DPF + SCCs
Linear Orbit Inc.	USA	SCCs
Lexware GmbH & Co. KG	Deutschland (EU)	Kein Drittlandtransfer

Twitter International UC / Irland / USA SCCs
X Corp.

Discord Netherlands BV / Niederlande / USA SCCs
Discord Inc.

§11 Cookies und ähnliche Technologien

Unser Onlineangebot verwendet ausschließlich technisch notwendige Cookies. Diese sind für den ordnungsgemäßen Betrieb des Onlineangebots erforderlich und werden ohne Einwilligung auf Grundlage von Art. 6 Abs. 1 lit. f DSGVO i. V. m. § 25 Abs. 2 Nr. 2 TDDDG gesetzt. Werbecookies, Tracking- oder Analyse-Cookies werden nicht eingesetzt.

Konkret setzen wir Session-Cookies zur Aufrechterhaltung Ihrer Anmeldung sowie CSRF-Token zum Schutz vor unbefugten Zugriffen ein. Beide Technologien sind ausschließlich für die Dauer Ihrer Sitzung aktiv und werden nach dem Abmelden automatisch gelöscht.

§12 Speicherdauer

Personenbezogene Daten werden nur so lange gespeichert, wie es für den jeweiligen Verarbeitungszweck erforderlich ist oder gesetzliche Aufbewahrungsfristen bestehen:

Datenkategorie	Speicherdauer
Kontodaten	Bis zur Löschung auf Antrag
Chatbot-Verläufe	Bis zur Löschung auf Antrag, maximal 3 Jahre
Support-Kommunikation	3 Jahre (§ 195 BGB)
Zugriffsprotokolle (Server-Logs)	14 Tage, danach Anonymisierung
Rechnungs- und Zahlungsdaten	10 Jahre (§ 147 AO, § 257 HGB)
Geschäftliche E-Mail-Kommunikation	6–10 Jahre je nach Inhalt (§ 147 AO / § 257 HGB)

§13 Ihre Rechte als betroffene Person

Als betroffene Person stehen Ihnen gegenüber dem Verantwortlichen die folgenden Rechte zu. Zur Geltendmachung wenden Sie sich bitte an: dataprotection@neoprotect.net.

Recht	Grundlage	Inhalt
-------	-----------	--------

Auskunft	Art. 15 DSGVO	Bestätigung über Verarbeitung und Kopie der personenbezogenen Daten
Berichtigung	Art. 16 DSGVO	Korrektur unrichtiger oder unvollständiger personenbezogener Daten
Löschung	Art. 17 DSGVO	Löschung, sofern keine Aufbewahrungspflichten entgegenstehen
Einschränkung	Art. 18 DSGVO	Beschränkung der Verarbeitung unter bestimmten Voraussetzungen
Datenübertragbarkeit	Art. 20 DSGVO	Herausgabe in maschinenlesbarem Format
Widerspruch	Art. 21 DSGVO	Widerspruch gegen auf lit. f gestützte Verarbeitungen
Widerruf	Art. 7 Abs. 3 DSGVO	Widerruf erteilter Einwilligungen mit Wirkung für die Zukunft
Beschwerde	Art. 77 DSGVO	Beschwerde bei der zuständigen Aufsichtsbehörde

Die für uns zuständige Datenschutzaufsichtsbehörde ist das Bayerisches Landesamt für Datenschutzaufsicht (BayLDA), Promenade 27, 91522 Ansbach <https://www.lida.bayern.de>. Das Auskunftsrecht nach Art. 15 DSGVO / GDPR können Sie bequem per Self-Service unter <https://panel.neoprotect.net/profile> über die Funktion „GDPR Export“ ausüben - dies ist die schnellste Methode.

Löschanträge nach Art. 17 DSGVO / GDPR richten Sie bitte per E-Mail an dataprotection@neoprotect.net mit dem Betreff „GDPR Data removal“; eine Identitätsprüfung kann erforderlich sein. Alle übrigen Anfragen richten Sie bitte an dataprotection@neoprotect.net. Wir beantworten Ihre Anfragen unverzüglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags. Diese Frist kann bei komplexen oder zahlreichen Anfragen um bis zu zwei weitere Monate verlängert werden; über eine solche Verlängerung sowie deren Gründe informieren wir Sie innerhalb eines Monats nach Eingang des Antrags (Art. 12 Abs. 3 DSGVO / GDPR).

§14 Datensicherheit und technisch-organisatorische Maßnahmen

Wir treffen nach Art. 32 DSGVO geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten:

- Verschlüsselte Datenübertragung mittels TLS/HTTPS
- Verschlüsselte Speicherung sensibler personenbezogener Daten (insbesondere Passwörter)
- Strikt rollenbasiertes Berechtigungskonzept (Need-to-know-Prinzip)
- Regelmäßige Sicherheitsupdates und systematisches Patch-Management
- Vertraulichkeitsvereinbarungen mit allen Personen, die Zugang zu personenbezogenen Daten haben

- Regelmäßige interne Datenschutzschulungen
- Protokollierung von Zugriffen auf besonders sensible Datenbereiche
- Datensicherungskonzept und regelmäßige Backups

§15 Änderung dieser Datenschutzerklärung

Wir behalten uns vor, diese Datenschutzerklärung anzupassen, wenn sich gesetzliche Anforderungen, eingesetzte Tools oder Verarbeitungstätigkeiten ändern. Die jeweils aktuelle Version ist stets unter <https://neoprotect.net/privacy> abrufbar. Über wesentliche Änderungen informieren wir Sie per E-Mail oder durch einen deutlichen Hinweis auf unserem Onlineangebot vor dem Inkrafttreten.

Diese Datenschutzerklärung wird in deutscher Sprache verfasst. Die deutschsprachige Fassung ist die allein verbindliche Version. Übersetzungen dienen ausschließlich Informationszwecken.

Privacy Policy (English translation)

NOTE: This English translation is provided for informational purposes only. The legally binding version is the German version above. (see §15)

This policy supplements the legal notice (available at <https://neoprotect.net/imprint>) and the General Terms and Conditions (available at <https://neoprotect.net/terms>).

With the following privacy policy, we wish to inform you about the types of your personal data we process, for which purposes and to what extent.

This privacy policy applies to all processing of personal data carried out by us, both in the course of providing our services and in particular on our websites, in mobile applications, and within external online presences such as our social media profiles (hereinafter collectively referred to as the “online offering”). The online offering also includes our password-protected members' area (hereinafter the “Panel”).

The terms used are not gender-specific.

§1 Controller

The controller within the meaning of the GDPR and the BDSG (German Federal Data Protection Act) is:

NeoProtect GmbH
Ulrichsberger Straße 17
94469, Deggendorf
Germany

Local Court (Amtsgericht): Deggendorf HRB 6544
Registered office: Deggendorf
Managing Directors: Kilian Pronold, Noah Kolossa
E-mail: dataprotection@neoprotect.net
Phone: +49 991 99993744
Website: <https://neoprotect.net>

§2 Data Protection Officer

As of now, no data protection officer (DPO) has been appointed. Please address data protection inquiries directly to the contact address stated under No. 1. We continuously review whether the statutory obligation to appoint a DPO pursuant to Art. 37 GDPR in conjunction with § 38 BDSG applies to our company.

§3 Registration and User Account

3.1 Data Collected

When you register for our online offering, we process the following personal data:

- First and last name
- E-mail address
- Password (stored exclusively in encrypted form (hash))
- Company name and address (if provided)
- IP address and timestamp of registration

3.2 Purpose and Legal Basis

The processing serves the establishment and performance of the user agreement (Art. 6(1)(b) GDPR) as well as compliance with legal obligations (Art. 6(1)(c) GDPR).

3.3 Consent Log upon Registration

In the course of registration, you expressly agree to our General Terms and Conditions (GTC) and to this privacy policy. This consent is logged with a timestamp and IP address. It can be withdrawn at any time with effect for the future; the lawfulness of the processing carried out up to the point of withdrawal remains unaffected.

3.4 Storage Period

Account data is stored for the duration of the user relationship. The user account and the associated personal data are deleted exclusively upon the user's express request, which can be submitted either via the account settings or by written request to dataprotection@neoprotect.net. Upon receipt of a deletion request, the account is completely deleted within the statutory period, provided that no statutory retention periods conflict with this. Data subject to statutory retention obligations (e.g., invoice data pursuant to § 147 AO (German Fiscal Code)) is stored until the expiry of the respective period and subsequently deleted.

§4 Use of the Online Offering and the Panel

When you use our online offering, technical access data is collected automatically. This includes the IP address, browser type and version, operating system, pages and functions accessed, date and time of access, and session IDs. The processing is carried out to ensure technical operation, for troubleshooting, and to protect against misuse (Art. 6(1)(f) GDPR). A combination with other personal data takes place only insofar as this is necessary for security or contract performance.

§5 AI-supported Chatbot (Amazon Bedrock / Claude)

5.1 General Information and Transparency

The AI-supported assistant is a central communication channel of our customer support and is available on our online offering both on publicly accessible pages and within the Panel. When a support request is initiated, support is regularly provided first via the AI-supported assistant. Unregistered users, as well as registered users who have not consented to the use of AI, may alternatively obtain support without using the AI assistant by email via the addresses stated on our website. Details on the legal basis and the alternatives are set out in Section 5.4.

During every interaction, the chatbot is unmistakably identified as an AI system – at no point is it a conversation with a human employee. This labelling obligation arises from Art. 50(1) of

the AI Regulation (Regulation (EU) 2024/1689, “EU AI Act”) as well as the transparency principle under Art. 5(1)(a) in conjunction with Art. 13 GDPR.

Before first use, a notice is displayed informing about the use of AI and the associated data processing, and referring to this privacy policy. Use of the support requires acknowledgement of this notice.

Recommendation: Please do not enter any particularly sensitive personal data into the chatbot – in particular no health data, bank details, identity document data, or passwords.

5.2 Technology Provider

To operate the chatbot, we use the service **Amazon Bedrock** provided by Amazon Web Services EMEA SARL (see Section 8.5 and 10). Language models from Anthropic (Claude) are executed via Amazon Bedrock. Processing takes place exclusively on AWS infrastructure; Anthropic has no direct access to the data transmitted in the course of using the chatbot. The data processing agreement (DPA) concluded with AWS pursuant to Art. 28 GDPR also covers the use of Amazon Bedrock.

5.3 Data Processed

In the course of using the chatbot, the following data is transmitted to the service:

- Your inputs (messages and requests) in the chat
- Session-related context information, insofar as required for generating the response
- Metadata (timestamp, session ID)
- Technical service configuration data for error detection of the service (no personal data)

For non-logged-in users, no personal data beyond this is processed or linked to a user account.

5.4 Legal Basis

For **logged-in users**, processing is based on Art. 6(1)(f) GDPR. Our legitimate interest lies in providing customer support efficiently, scalably, and with consistent quality through the use of an AI-powered assistance system. The chatbot is not a mandatory component of the contract but rather a recommended communication channel; alternative contact options are available via the email addresses listed on our website.

As part of a documented balancing of interests, we have taken into account that (i) processing is limited to what is necessary for providing support, (ii) no automated decisions within the meaning of Art. 22 GDPR are made, (iii) the user is informed transparently in advance about the use of AI, and (iv) chat logs can be deleted at any time upon request. Your right to object pursuant to Art. 21 GDPR remains unaffected by this.

For **non-logged-in users**, processing is carried out on the basis of the consent expressly granted pursuant to Art. 6(1)(a) GDPR. Before first use of the chatbot, non-logged-in users are shown a notice informing about the use of AI, the data processed, and the session-based limitation of storage, and referring to this privacy policy. The chatbot can only be used after active confirmation of this notice. Consent is logged on a session-related basis. It can be refused or withdrawn at any time by ending the session or by not using the chatbot; a permanent association with a person does not take place without registration. For logged-in users, a notice is likewise displayed before first use informing about the use of AI and referring to this privacy policy.

5.5 Third-Country Transfer

We use Amazon Bedrock with a region-bound endpoint in the AWS region eu-central-1 (Frankfurt, Germany); cross-region or global routing of inference is disabled for this service. The processing of the chatbot content (prompts and responses) therefore takes place within the European Economic Area. The Anthropic models provided via Amazon Bedrock run on AWS-managed infrastructure; Anthropic has no access to the content transmitted in the course of using the chatbot (see Section 5.2). A residual risk of governmental access on the basis of US law (in particular the CLOUD Act) cannot be entirely excluded where a US group operates the infrastructure; we address this risk through the safeguards agreed with AWS and technical protective measures (see Section 10). Insofar as a transfer to a third country is required in an individual case for supplementary technical processing (e.g. operation, troubleshooting or support), such transfer takes place only on the basis of the safeguards set out in Section 10.

5.6 Automated Decision-Making

The chatbot does not make any automated decisions that produce legal effects concerning you or similarly significantly affect you within the meaning of Art. 22 GDPR. All generated responses are to be understood as informational offerings and do not replace legal, medical, or professional advice.

5.7 Storage Period

Chat histories of logged-in users are stored for the duration of the user relationship, but no longer than 3 years. Deletion takes place upon express request via the account settings or by e-mail to support@neoprotect.net with the subject "GDPR Data removal"; upon receipt of the request, deletion takes place within the statutory period.

Chat histories of non-logged-in users are processed exclusively for the duration of the session and are not stored permanently. After the session ends, the conversation data is deleted.

§6 Payment Processing

6.1 Stripe

For payment processing, we use:

Stripe Payments Europe, Ltd. 1 Grand Canal Street Lower, Grand Canal Dock, Dublin D02 H210, Ireland Data protection information: <https://stripe.com/de/privacy>

Your payment data (e.g., credit card number, IBAN) is transmitted directly to Stripe; we ourselves do not store any complete payment data. Stripe acts as an independent controller for parts of the processing. For third-country transfers to the USA, Stripe relies on the EU-U.S. Data Privacy Framework (DPF) as well as SCCs. Legal basis: Art. 6(1)(b) GDPR.

6.2 PayPal

Alternatively, we offer payment via PayPal:

PayPal (Europe) S.à r.l. et Cie, S.C.A. 22-24 Boulevard Royal, L-2449 Luxembourg Data protection information: <https://www.paypal.com/de/webapps/mpp/ua/privacy-full>

If you select PayPal, you will be redirected to their platform. PayPal processes your personal data as an independent controller. Intra-group transfer to the USA takes place on the basis of DPF and SCCs. Legal basis: Art. 6(1)(b) GDPR.

§7 Internal Tools and Contractual Agents

We use the following software tools, to which only employees of NeoProtect GmbH have access. All employees are bound to confidentiality by confidentiality agreements (NDAs). This measure is part of our technical and organizational protective measures pursuant to Art. 32 GDPR.

In addition to permanently employed staff, we use external contractors (freelancers) to a limited extent, who in the course of their work may have access to internal systems and – insofar as necessary for their tasks – to personal data similar to that of employees. Data processing agreements pursuant to Art. 28 GDPR and confidentiality agreements (NDAs) are concluded with these persons. Access is granted exclusively on a need-to-know basis. Legal basis: Art. 6(1)(f) GDPR.

7.1 Slack (internal communication)

Slack (operator: Salesforce, Inc., 415 Mission Street, San Francisco, CA 94105, USA) is used exclusively for internal communication. In the course of support processes, personal data relating to user inquiries may be indirectly discussed. A DPA pursuant to Art. 28 GDPR exists with Salesforce/Slack; third-country transfers to the USA take place on the basis of DPF and SCCs. Data protection information: <https://slack.com/trust/privacy>. Legal basis: Art. 6(1)(f) GDPR (legitimate interest in efficient internal communication).

7.2 Google Workspace (e-mail, documents, calendar, telephony) and Google Places API (address validation)

We use Google Workspace (operator: Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland; subsidiary of Google LLC, USA) for e-mail, document editing, calendar, as well as telephony and voice communication. Personal data may be contained in business communication.

In addition, we use the Google Places API (Google Maps Platform) for server-side validation of address entries. In this process, the address data entered is transmitted exclusively from our server to the Google API; a direct connection between your browser and Google servers does not take place within the scope of this function. Only the data necessary for address validation (the address components entered) is transmitted – no personal data beyond this. A DPA pursuant to Art. 28 GDPR exists with Google; third-country transfers to the USA take place on the basis of DPF and SCCs. Data protection information: <https://policies.google.com/privacy>. Legal basis: Art. 6(1)(b) and (f) GDPR.

7.3 Linear (project management)

Linear (operator: Linear Orbit Inc., USA) is used by us for internal task and project management. Tickets may indirectly contain personal data relating to user inquiries. A DPA pursuant to Art. 28 GDPR exists with Linear; third-country transfers to the USA take place on the basis of SCCs. Data protection information: <https://linear.app/privacy>. Legal basis: Art. 6(1)(f) GDPR (legitimate interest in efficient project management).

7.4 Lexoffice / Lexware (accounting and invoicing)

We use Lexoffice (operator: Lexware GmbH & Co. KG or Haufe-Lexware GmbH & Co. KG, Munzinger Straße 9, 79111 Freiburg im Breisgau, Germany) for accounting and to fulfil record-keeping obligations under tax and commercial law. In this process, we process master data of our customers (name, address, and, where applicable, VAT identification

number) as well as invoice and payment data.

The data processing takes place on servers in Germany; no third-country transfer takes place. A data processing agreement (DPA) pursuant to Art. 28 GDPR exists with Lexware.

Data protection information: <https://www.lexware.de/datenschutz/>.

Legal basis: Art. 6(1)(b) GDPR (contract performance) as well as Art. 6(1)(c) GDPR in conjunction with § 147 AO, § 257 HGB (compliance with statutory retention and record-keeping obligations).

7.5 DocuSeal (electronic signature and document management)

We use DocuSeal (operator: DocuSeal LLC, 332 S Michigan Ave, Suite 121 #5896, Chicago IL 60604) for the creation, dispatch, and legally compliant electronic signing of documents (e.g., contracts, order confirmations, NDAs). In this process, we process master data of the signing parties (in particular name, e-mail address, and, where applicable, company affiliation) as well as the document contents and signature metadata (e.g., timestamp, IP address at the time of signing).

We use the European variant (docuseal.eu); the data processing takes place on servers within the EU/EEA, and no third-country transfer takes place. A data processing agreement (DPA) pursuant to Art. 28 GDPR exists with DocuSeal.

Data protection information: <https://www.docuseal.com/privacy>.

Legal basis: Art. 6(1)(b) GDPR (contract performance) as well as Art. 6(1)(f) GDPR (legitimate interest in efficient and legally compliant electronic document handling).

§8 Hosting and Technical Infrastructure

To operate our online offering, we use external hosting and infrastructure providers on whose servers or networks personal data (e.g., server logs, uploaded files, database contents) is stored or transmitted. We have concluded data processing agreements (DPAs) pursuant to Art. 28 GDPR with all of the providers named below.

8.1 Hetzner (primary server infrastructure)

Hetzner Online GmbH Industriestr. 25, 91710 Gunzenhausen, Germany Data protection information: <https://www.hetzner.com/de/legal/privacy-policy>

Hetzner is a German company with data centers exclusively in Germany and Finland (EU/EEA). No third-country transfer of personal data takes place. Database contents, application data, and server logs may be stored on the Hetzner servers. Legal basis: Art. 6(1)(b) and (f) GDPR.

8.2 OVHCloud (server infrastructure)

OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken, Germany (subsidiary of OVH SAS, 2 rue Kellermann, 59100 Roubaix, France) Data protection information:

<https://www.ovhcloud.com/de/personal-data-protection/>

OVHcloud operates data centers in Germany, France, and other EU/EEA locations. A third-country transfer outside the EEA does not take place by default. Application data and backups may be stored on OVH infrastructure. Legal basis: Art. 6(1)(b) and (f) GDPR.

8.3 Cloudflare (CDN and network security)

Cloudflare, Inc., 101 Townsend St., San Francisco, CA 94107, USA Data protection information: <https://www.cloudflare.com/de-de/privacypolicy/>

We use Cloudflare as a Content Delivery Network (CDN) for faster delivery of our web content as well as for protection against DDoS attacks and other threats. The traffic between your browser and our online offering is routed through Cloudflare's global network; in this process, Cloudflare may process technical access data (in particular IP addresses). The third-country transfer to the USA takes place on the basis of the DPF and the SCCs pursuant to Art. 46(2)(c) GDPR. For users in the EEA, personal data is preferentially processed in European data centers. Legal basis: Art. 6(1)(f) GDPR (legitimate interest in the secure and performant provision of the online offering).

8.4 hCaptcha (bot and abuse detection)

Intuition Machines, Inc., 350 Alabama St, San Francisco, CA 94110, USA Data protection information: <https://www.hcaptcha.com/privacy>

To protect our forms (in particular registration and login) against automated access, bots, and abuse, we use the hCaptcha service provided by Intuition Machines, Inc. When hCaptcha is used, the service automatically analyzes the visitor's behavior based on various characteristics (in particular IP address, browser and device information, and interaction data such as mouse movements) in order to distinguish between human users and automated requests. The analysis runs in the background; for this purpose, a script is loaded from hCaptcha's servers, whereby technical access data (in particular your IP address) is transmitted to Intuition Machines. The third-country transfer to the USA takes place on the basis of the EU-U.S. Data Privacy Framework (DPF) and, supplementarily, the Standard Contractual Clauses (SCCs) pursuant to Art. 46(2)(c) GDPR. Legal basis: Art. 6(1)(f) GDPR (legitimate interest in protecting our online offering against bots, spam, and abusive automated use).

8.5 Amazon Web Services - AWS (CDN and object storage)

Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855 Luxembourg (subsidiary of Amazon.com, Inc., 410 Terry Ave. North, Seattle, WA 98109, USA) Data protection information: <https://aws.amazon.com/de/privacy/>

We use AWS as a Content Delivery Network (Amazon CloudFront) for the performant delivery of static content, as object storage (Amazon S3) for the secure storage of files and media, and as AI inference infrastructure (Amazon Bedrock) for operating the chatbot (see Section 5). We also use AWS for storing any software versions of our products (Amazon ECR) in order to implement autonomous version management, as well as for internal proxy activities for, among other things, internal SSH and VPN services (Amazon EC2) in order to comply with self-imposed security standards. We use AWS services primarily in the region eu-central-1 (Frankfurt, Germany). Third-country transfers to the USA cannot be entirely ruled out within the framework of the intra-group infrastructure; they take place on the basis of the DPF and the SCCs pursuant to Art. 46(2)(c) GDPR. Legal basis: Art. 6(1)(b) and (f) GDPR.

8.6 Atlassian Statuspage (status page, system status display)

Atlassian Network Services, Inc., 350 Bush Street, Floor 13, San Francisco, CA 94104, USA Data protection information: <https://www.atlassian.com/legal/privacy-policy>

When our Panel is loaded, status information is retrieved from Atlassian's servers and displayed on our page. In doing so, your browser may establish a direct connection to

Atlassian's infrastructure, whereby Atlassian may process technical access data – in particular your IP address.

We ourselves do not transmit any personal data to Atlassian. Should you wish to sign up for e-mail notifications of status changes, this is done exclusively through your voluntary input on the Atlassian Statuspage; the processing of this data lies within the sole area of responsibility of Atlassian.

As Atlassian is based in the USA, a third-country transfer may occur during data processing. This takes place on the basis of the Standard Contractual Clauses (SCCs) pursuant to Art. 46(2)(c) GDPR as well as the EU-U.S. Data Privacy Framework (DPF).

Legal basis: Art. 6(1)(f) GDPR (legitimate interest in transparent communication of the system status to our users).

§9 Presences on Social Networks

We maintain public profiles on the social networks named below and publish organic content as well as paid advertisements there. A technical integration of these platforms into our online offering (e.g., through plugins, tracking pixels, or social buttons) does not take place. As soon as you visit the respective platforms or interact with our profiles, the platform operators process your personal data on their own responsibility in accordance with their own privacy policies. We have no influence on this processing. We recommend reading the privacy notices of the respective platforms.

9.1 Instagram and Facebook (Meta Platforms)

Meta Platforms Ireland Limited 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Ireland Data protection information: <https://www.facebook.com/privacy/policy>

On our Meta pages (Instagram / Facebook), we publish organic posts as well as paid advertisements. In the course of placing advertisements, Meta uses its own targeting mechanisms based on the user data stored at Meta; in doing so, we do not transmit any personal data of our own users to Meta. For the processing of page statistics (Page Insights), there is joint controllership pursuant to Art. 26 GDPR between us and Meta. Meta assumes primary responsibility for fulfilling data subject rights. Third-country transfers to the USA take place on the basis of DPF and SCCs. Legal basis: Art. 6(1)(f) GDPR. The key provisions of the agreement can be viewed at https://www.facebook.com/legal/terms/page_controller_addendum. Meta assumes primary responsibility for ensuring that data subjects' rights regarding Page Insights data are upheld. Notwithstanding this, you may also exercise your rights with us; we will forward your request to Meta if necessary.

9.2 LinkedIn

LinkedIn Ireland Unlimited Company Wilton Place, Dublin 2, Ireland Data protection information: <https://www.linkedin.com/legal/privacy-policy>

On our LinkedIn company page, we publish organic content as well as paid advertisements (LinkedIn Ads). For page statistics (Page Analytics), there is joint controllership pursuant to Art. 26 GDPR with LinkedIn Ireland. Third-country transfers to the USA take place via DPF and SCCs. Legal basis: Art. 6(1)(f) GDPR. The key provisions of the joint controller agreement can be viewed at <https://www.linkedin.com/legal/page-joint-controller-addendum>

9.3 X (formerly Twitter)

We maintain a public profile on the platform X. The operator for users in the EEA is Twitter International Unlimited Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07, Ireland (parent company: X Corp., USA). Data protection information: <https://x.com/de/privacy>. As soon as you visit our profile or interact with our posts, the platform operator processes your personal data on its own responsibility in accordance with its own privacy policies; we have no influence on this processing. A technical integration into our online offering (plugins, tracking pixels, social buttons) does not take place. Third-party transfers to the USA take place on the basis of the Standard Contractual Clauses (SCCs) pursuant to Art. 46(2)(c) GDPR. Legal basis: Art. 6(1)(f) GDPR (legitimate interest in public self-presentation and communication).

9.4 Discord

We operate a public Discord server that serves our users as a community and support channel. The operator is Discord Netherlands BV (European establishment; parent company: Discord Inc., 444 De Haro Street, San Francisco, CA 94107, USA). Data protection information: <https://discord.com/privacy>. When you join our server or communicate there, Discord processes the data arising in this context (in particular username, user ID, message contents, connection data) as an independent controller in accordance with its own privacy policies. Insofar as we administer the server and process personal data in this context (e.g., to respond to inquiries or for moderation), this is done on the basis of Art. 6(1)(f) GDPR (legitimate interest in community support and assistance); participation is voluntary. Please do not enter any particularly sensitive data in the chat. Third-party transfers to the USA take place on the basis of the Standard Contractual Clauses (SCCs) pursuant to Art. 46(2)(c) GDPR.

9.5 Notes on Advertising

When placing advertisements, we transmit to the platforms exclusively aggregated target group definitions (e.g., industry, interests, geographic region) – no individual personal data of our users or customers. The platforms display our advertisements to their own user base based on these specifications. For questions regarding the platform-side data processing, we refer to the respective privacy notices.

§10 Third-Country Transfers

Several of the providers we use are based in the USA. Depending on the provider, we base transfers to the USA on one of the following two grounds: (i) the EU-U.S. Data Privacy Framework, for which the EU Commission issued an adequacy decision pursuant to Art. 45 GDPR on 10 July 2023, provided the respective recipient is actively certified under the DPF; or (ii) the European Commission's Standard Contractual Clauses as appropriate safeguards pursuant to Art. 46 GDPR, supplemented by technical and organisational protective measures. The transfer legal basis applicable to each provider is set out in the table below.

Provider	Registered Office	Transfer Legal Basis
Hetzner Online GmbH	Germany (EU)	No third-country transfer
OVH GmbH / OVH SAS	Germany / France (EU)	No third-country transfer

Provider	Registered Office	Transfer Legal Basis
Cloudflare, Inc.	USA	DPF + SCCs
Intuition Machines, Inc. (hCaptcha)	USA	DPF + SCCs
Amazon Web Services EMEA	Luxembourg / USA	DPF + SCCs
Anthropic, PBC	USA	SCCs (Art. 46(2)(c) GDPR)
Meta Platforms Ireland	Ireland / USA	DPF + SCCs
LinkedIn Ireland	Ireland / USA	DPF + SCCs
Stripe Payments Europe	Ireland / USA	DPF + SCCs
PayPal (Europe)	Luxembourg / USA	DPF + SCCs
Salesforce / Slack	USA	DPF + SCCs
Google LLC / Google Ireland	USA / Ireland	DPF + SCCs
Linear Orbit Inc.	USA	SCCs
Lexware GmbH & Co. KG	Germany (EU)	No third-country transfer
Twitter International UC / X Corp.	Ireland / USA	SCCs
Discord Netherlands BV / Discord Inc.	Netherlands / USA	SCCs

§11 Cookies and Similar Technologies

Our online offering uses exclusively technically necessary cookies. These are required for the proper operation of the online offering and are set without consent on the basis of Art. 6(1)(f) GDPR in conjunction with § 25(2) No. 2 TDDDG (German Telecommunications Digital Services Data Protection Act). No advertising cookies, tracking cookies, or analytics cookies are used.

Specifically, we use session cookies to maintain your login as well as CSRF tokens to protect against unauthorized access. Both technologies are active exclusively for the duration of your session and are automatically deleted after you log out.

§12 Storage Period

Personal data is stored only for as long as is necessary for the respective processing purpose or for as long as statutory retention periods exist:

Data Category	Storage Period
Account data	Until deletion upon request
Chatbot histories	Until deletion upon request, maximum 3 years
Support communication	3 years (§ 195 BGB)
Access logs (server logs)	14 days, then anonymization
Invoice and payment data	10 years (§ 147 AO, § 257 HGB)
Business e-mail communication	6–10 years depending on content (§ 147 AO / § 257 HGB)

§13 Your Rights as a Data Subject

As a data subject, you have the following rights vis-à-vis the controller. To exercise them, please contact: dataprotection@neoprotect.net.

Right	Basis	Content
Access	Art. 15 GDPR	Confirmation of processing and a copy of the personal data
Rectification	Art. 16 GDPR	Correction of inaccurate or incomplete personal data
Erasure	Art. 17 GDPR	Erasure, provided that no retention obligations conflict with this
Restriction	Art. 18 GDPR	Restriction of processing under certain conditions
Data portability	Art. 20 GDPR	Provision in a machine-readable format
Objection	Art. 21 GDPR	Objection to processing based on (f)
Withdrawal	Art. 7(3) GDPR	Withdrawal of consent given, with effect for the future
Complaint	Art. 77 GDPR	Complaint to the competent supervisory authority

The supervisory authority for data protection responsible for us is the Bavarian State Office for Data Protection Supervision (Bayerisches Landesamt für Datenschutzaufsicht, BayLDA), Promenade 27, 91522 Ansbach <https://www.lida.bayern.de>.

You can conveniently exercise the right of access pursuant to Art. 15 GDPR via self-service at <https://panel.neoprotect.net/profile> using the “GDPR Export” function – this is the fastest method.

Please send erasure requests pursuant to Art. 17 GDPR by e-mail to dataprotection@neoprotect.net with the subject “GDPR Data removal”; an identity check may be required. Please address all other inquiries to dataprotection@neoprotect.net. We will respond to your inquiries without undue delay, in any case within one month of receipt of the request. This period may be extended by up to two further months in the case of complex or numerous requests; we will inform you of any such extension and the reasons for it within one month of receipt of the request (Art. 12(3) GDPR).

§14 Data Security and Technical and Organizational Measures

In accordance with Art. 32 GDPR, we take appropriate technical and organizational measures to ensure a level of protection appropriate to the risk:

- Encrypted data transmission using TLS/HTTPS
- Encrypted storage of sensitive personal data (in particular passwords)
- Strictly role-based authorization concept (need-to-know principle)
- Regular security updates and systematic patch management
- Confidentiality agreements with all persons who have access to personal data
- Regular internal data protection training
- Logging of access to particularly sensitive data areas
- Data backup concept and regular backups

§15 Amendment of this Privacy Policy

We reserve the right to adapt this privacy policy if statutory requirements, the tools used, or processing activities change. The current version is always available at <https://neoprotect.net/privacy>. We will inform you of material changes by e-mail or by means of a clearly visible notice on our online offering before they take effect.

This privacy policy is drawn up in the German language. The German-language version is the sole binding version. Translations serve informational purposes only.